SUPPORTING STATEMENT
U.S. Department of Commerce
Director, Office of Security (OSY)
Foreign National Request Form A

A. JUSTIFICATION

This Information Collection Request is submitted to the Office of Management and Budget (OMB) for approval consistent with the Paperwork Reduction Act (44 USC §3501).

1. Explain the circumstances that make the collection of information necessary.

The mission of the Department is to create the conditions for economic growth and opportunity. The Department of Commerce promotes job creation and economic growth by ensuring fair and reciprocal trade, providing the data necessary to support commerce and constitutional democracy, and fostering innovation by setting standards and conducting foundational research and development.

The Department of Commerce (DOC) has an imperative to know the identity of individuals seeking access to DOC facilities or activities for safety, security, and compliance with Federal laws and regulations.

International engagement is an essential component of the Department's mission intended to promote U.S. innovation and industrial competitiveness by advancing science, standards and technology in ways that enhance economic security and improve quality of life. To advance this mission, the Department invites foreign individuals from universities, other institutions, corporations and other international organizations to conduct research at Department facilities. These Foreign Nationals (FN) include foreign and domestic guest researchers, research associates, contractors, and other non-federal employees who require access to Department facilities and resources to engage in collaborate efforts. The activities of range from highly-technical work in laboratories to construction and maintenance of facilities.

FNs support a broad range of collaborative initiatives across the Department working collaboratively with Department scientists on research and development projects of mutual interest or to transfer NIST "know-how," methodologies, procedures, and best practices. FNs are given access to Department facilities to advance initiatives of benefit to the Federal government but likewise entails a level of security risk. Department research and development sites include sophisticated equipment, proprietary information, sensitive and classified information, and information related to U.S. businesses. These sites have lasers, reactors, hazardous materials, and other safety concerns that are a necessary part of research. In many areas the advanced research performed is controlled by export control regulations and requires background information to ensure compliance. The Department hosted approximately 12,000 FNs visitors and guest researchers between July 2017 and July 2018 in support of its mission.

Providing access to these sites and equipment involves a risk for which the DOC must ensure safety of both the FNs and Department employees. This requires an understanding of the

background and qualifications of FNs accessing Department facilities and resources. In addition, intellectual property developed during research is controlled by several laws and it is important understand the background and affiliation of FNs to accurately consider questions of intellectual property and government use rights resulting from work performed in collaboration with Department scientists and researchers.

The Office of Security (OSY) serves to protect personnel, facilities, missions and information by collaborating with key leaders, decision-makers, and stakeholders across all operating units to effectively mitigate security risks throughout the Department of Commerce (Department) via issuance of Department-wide security policies and the customized application of a multi-disciplined security program extending from the Headquarters to our various operating units. OSY establishes and enforces policies and procedures for conducting background investigations and granting security clearances; safeguarding classified and sensitive documents and information; protecting Department personnel, facilities, missions and property; assessing threats and determining risks to Departmental assets; ensuring proper communications security; providing guidance to Departmental offices and operating units on security-related matters; and, ensuring compliance with security policies and procedures. Specifically, OSY conducts investigations and analyses to identify and/or assess critical threats to the Department's mission, operations or activities, and prevents or mitigates such threats from adversely affecting Department personnel, facilities, property or assets through strategic and tactical approaches.

Due to the increasing diversity of foreign national participation within the Department, considerable efforts were made by OSY to baseline requirements as means to define uniform program standards as well as expand current guidance beyond foreign visitor control. The *DOC Foreign National Request Form A* (Form A) is designed for investigative purposes as a single resource document and ready tool for use by Department bureaus, staff offices and operating units to increase efficiency and mitigate variance in foreign access management and information registration requirements needed to achieve risk-based determinations of physical and logical access by FNs to Department facilities and resources.

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

Information solicited by Form A will be used by Department bureaus and operating units for each FN. The information collected will be used for risk-based assessments of short term access or as partial completion towards long term guest research agreements and supporting security and background investigations for potential personal identity credential issuance in compliance with U.S. laws and regulations governing physical and logical access to federal facilities and information resources.

Collection methods vary across Department bureaus and operating units depending on implementation of either automated or paper-based business processes. Form A will be available as a fillable printable document on the OSY website (http://www.osec.doc.gov/osy/Forms/default.htm) permitting either digital collection or can be completed in writing to facilitate ease of use. The type of business processes employed (paper-based or automated), will determine the collection

instrument and methodology used Department bureaus and operating units. Form A may be transmitted to the FN for completion and return to the requestor in advance of arrival or completed in-person during on-boarding interviews with security personnel. Employer/home organization, address, sponsor name, sponsor address will be used to determine intellectual property rights but also have programmatic and statistical analysis uses such as reporting the number of FNs from a specific foreign country or sponsoring organization. Employment information has practical application such as providing Emergency personnel with quick access to employer or home organization contacts for emergency purposes.

Routinely, administrative support personnel will communicate in advance of the FNs arrival, and depending on the business employed by the bureau or operating unit, provide Form A as the data collection instrument for file or input into automated systems such as FNRS and NAIS. These systems route the information to operating unit stakeholders and administrators with equity in the project or programs selected for possible FN collaboration. FNs will be not allowed access to Department facilities or resources without approval. Following operating unit approval, FN information is routed to OSY Field Servicing Security Offices to determine if any additional processing or background investigation is required to facilitate final access determination. warranted. The data collected will be the basis for completing Office of Personnel Management (OPM) background investigation questionnaires consistent with OPM policy and guidelines.

The two OPM issued questionnaires used by Department bureaus and operating units for determinations of physical and logical access by FNs are the OFI-86C, "Special Agreement Check" and the SF-85, "Questionnaire for Non-Sensitive Positions." Form A information can be used to complete or verify the information included on the OFI-86C or facilitate data entry into the OPM Electronic Questionnaire for Investigations Processing (e-QIP) tool. OPM's e-QIP is an automated system that facilitates the processing of standard investigative forms for background processing. This input occurs outside Departmental systems previously mentioned. The FN is invited into e-QIP only after their nomination is approved by the operating unit and only when an investigation is necessary. Using e-QIP allows FNs to transmit their personal information in a private and secure manner. The associated Authorization and Release form for each OPM questionnaire provides the authority for the collection, purpose of the collection, routine uses and consequences of not providing information as required by 5 U.S.C. 5521(e)(3).

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.

The information collected will be filed for retention or input into independently developed and approved automated foreign access management systems or data bases such as the National Oceanic and Atmospheric Administration (NOAA), Foreign National Registration System (FNRS) and the National Institute of Standards and Technology (NIST), NIST Associates Information System (NAIS). The FNRS is designed to provide NOAA employees a single online location to enter and process the information needed to obtain determinations of access by FNs to NOAA facilities, ships, and airplanes. The NIST Associates Information System (NAIS) automates the preparation, review, and approval of all FN agreements, records, extensions, and security forms and tracks the review and acceptance of FNs nominated for access to NIST facilities and resources. Both automated systems are designed simplify the information

collection process by allowing for a single collection of data that is used on multiple forms therefore reducing transfer errors and decreasing time required.

The collected information is subsequently input into the Department SecurityManager™ system. SecurityManager™ is a suite of applications for an enterprise-wide management solution in support of the President's Management Agenda for E-Government and other Federal Agency performance and process reform goals. By utilizing this program, OSY headquarters and field office operations are better able to perform their support functions for the Secretary of Commerce and the Department in meeting national requirements under Executive Order (E.O.) 13467, as amended, Security Requirements for Government Employment, E.O. 12958 as amended, Classified National Security Information, and E.O. 12968, Access to Classified Information, among others.

The purpose of this system is to collect and maintain records of processing of personnel security-related clearance actions, to record suitability determinations, to record whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. Also, records may be used by the Department for adverse personnel actions such as removal from sensitive duties, removal from employment, denial to a restricted or sensitive area, and/or revocation of security clearance. The system also assists in capturing background investigations and adjudications; directing the clearance process for granting, suspending, revoking and denying access to classified information; directing the clearance process for granting, suspending, revoking and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of the Department; managing state, local and private-sector clearance programs and contractor suitability programs; determining eligibility for unescorted access to Department owned, occupied or secured facilities or information technology systems; and/or other activities relating to personnel security management responsibilities at the Department.

SecurityManager™ provides OSY personnel with the tools (hardware, software, and training) and access to the internal and external information resource necessary to perform their responsibilities. The system controls access to only those authorized as well as aids in the monitoring, assessment and response to security and emergency related incidents.

The information will be collected, maintained, and used in a way that is consistent with the applicable Department Chief Information Officer (CIO) Information Quality Guidelines and Standards. Only general demographic information may be released publicly— for example, for Congressional testimony or in a speech or remarks approved for public release to security, law enforcement, or government science or research fora for which professional interest in the character of international participation at Department sites and locations is germane.

Data exclusive to OPM background investigation questionnaires is excluded from collection as information not required by the FNRS and NAIS process.

4. <u>Describe efforts to identify duplication</u>.

The collected information is specific to each FN and is not available elsewhere. The Department's information collection process is designed to reduce and prevent duplication. Respondents can complete Form A as a primary information collection instrument for immediate

use, file or input to supporting Department systems or databases.

FN respondents will only need to complete Form A and appropriate OPM background investigation questionnaires once for the duration of the approved visit or appointment.

Existing systems such as the OPM e-QIP and the GSA USAccess program are separate and distinct data collection systems and generally not configured to complement near term access determinations by Department bureaus and operating units. The GSA USAccess program provides federal government agencies with identity credential solutions. This program is aligned with the Federal IT Shared Services Strategy which covers the use of shared services and the modernization of IT in the federal government and provides an efficient, economical and secure infrastructure to support agencies' credentialing needs. As stated previously, the information needed for the forms and agreements required as part of FN approval processes and the information needed for purposes of intellectual property rights are not collected in the USAccess program as that information is reviewed and adjudicated prior to the initiation of the personal identity verification credentialing process. Moreover, not all FNs are required to have a personal identity verification credential, and therefore will not need to provide information for use within USAccess. OSY Field Servicing Security Offices provide dedicated security support services to Department bureaus and operating units and play an integral role in the development of local procedures to ensure consistency and economy of scale for security programs across the Department. Recurring engagement between OSY and bureau and operating unit security stakeholders facilitates proactive coordination to mitigate duplication of efforts in response to emerging issues or needs.

5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.

This collection of information does not involve small businesses or other small entities.

6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.

The information will be collected in advance of FN arrival or as part of the routine on-boarding processes controlled by bureaus and operating units and may be updated if/when their agreement is extended (typically annually).

The information collected is critical to the administrative and security processing of FNs in direct support of Department mission success. Due to a variety visa, immigration, and related U.S. law enforcement requirements it is not possible to process FNs without collecting the data. Modifying the process to have FNs provide the information on multiple forms for individual purposes would result in additional burden on respondents to provide identical information. Data inconsistencies, increased errors, as well as the additional administrative burden upon OSY and Department bureaus and operating units would serve to only lengthen the time required to bring FNs on board and negatively impact operational effectiveness.

The Bayh-Dole Act of 1980 and Executive Order 12591 permit a university, business, or non-profit institution to elect to pursue ownership of an invention created under federally funded research projects in preference to the government. Lack of knowledge of the employer/home

organization of an FN will compromise the determination of intellectual property rights for both the FN and the Department. If this information is not collected or collected less frequently, the increased risk of unauthorized persons gaining undue access to secure Department facilities can be realized.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines.

Although, in an effort to meet mandated mission requirements, we are requesting an emergency approval; this information collection is consistent with OMB guidelines.

8. Provide information of the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

The Emergency *Federal Register* Notice soliciting public comment was published on August 21, 2018 (Volume 83, pg. 42253). No comments were received.

In addition, Commerce reached out to the Office of Security in other Federal agencies to obtain their views on this information collection prior to this submission.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

No payments or gifts will be provided.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

No assurances of confidentiality will be given. Department bureaus and operating units are governed by the provisions of 5 U.S.C. 522a (Privacy Act of 1974), and selected provisions of other Federal statutes, regulations, policies, and procedural guidelines. Department Rules of Behavior are not intended to supersede any such statutes, regulations, etc., nor are these rules intended to conflict with these pre-existing statutes and regulations. Rather, these rules of behavior are intended to enhance and further define the specific procedures each user must follow while accessing access control systems, consistent with Department Privacy, Security and Access Policies.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

There are no sensitive questions.

12. Provide an estimate in hours of the burden of the collection of information.

The Department estimates approximately 12,000 FNs will be processed per year. It is estimated that it will take 15 minutes to complete Form A as the identified collection instrument.

Therefore, the estimated total burden hours would be as follows:

12,000 x 15 minutes per response = 3,000 burden hours.

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in Question 12 above).

The estimated annual cost burden to respondents, excluding the value of the burden hours in Question 12, is $0.

14. Provide estimates of annualized cost to the Federal government.

DOC/OSY estimates that DOC personnel spend approximately 30 minutes reviewing and responding to each submission. DOC values its employees' time at $56/hour. The estimate of annualized cost to the Federal government is as follows:

12,000 guests and visitors/year * 30 minutes/submission * $56/hour = $336,000

Therefore, the Department estimates the annualized cost to the Federal government is **$336,000.**

15. Explain the reasons for any program changes or adjustments.

This is a new information collection.

16. For collections whose results will be published, outline the plans for tabulation and publication.

The results of this collection will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

Not applicable.

18. Explain each exception to the certification statement.

None.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection does not employ statistical methodology.